AF

| TRANSMITTAL OF APPEAL BRIEF (Large Entity) | Docket No. 200 |
|---|---|

In Re Application Of: **HOLLAR, MARK**

| Serial No. | Filing Date | Examiner | Group Art Unit |
|---|---|---|---|
| 09/711,000 | 11/9/2000 | ELISCA | 3621 |

Invention: **METHOD AND APPARATUS FOR DETERMINING DIGITAL A/V CONTENT DISTRIBUTION TERMS BASED ON DETECTED PIRACY LEVELS**

TO THE COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **AUG. 18, 2004**

The fee for filing this Appeal Brief is: **$330.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **13-0762**

*Signature*

Dated: 9/9/04

**JIM SALTER**
**PATENT COUNSEL**
**MACROVISION CORPORTION**
**2830 DE LA CRUZ BLVD**
**SANTA CLARA**
**CA 95050**

**REG NO 35668**

I certify that this document and fee is being deposited on 9/10/04 with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*Signature of Person Mailing Correspondence*

**ANNE KILLINGSWORTH**

*Typed or Printed Name of Person Mailing Correspondence*

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re Patent Application of: | |
| Hollar, Mark A. | **ON APPEAL TO THE BOARD OF APPEALS** |
| Applic.Serial No.: 09/711,000 | |
| Filed: 11/09/2000 | |
| For: METHOD AND APPARATUS FOR DETERMINING DIGITAL A/V CONTENT DISTRIBUTION TERMS BASED ON DETECTED PIRACY LEVELS | Examiner: Elisca, Pierre E. |
| | Group Art Unit: 3621 |
| | Confirmation No.: 6001 |

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## APPEAL BRIEF

Sir:

This is an appeal from the Final Rejection, dated July 21, 2004 for the above-identified patent application.

## REAL PARTY IN INTEREST

The real party in interest of the above-identified patent application is its Assignee, Macrovision Corporation, incorporated in the state of Delaware and having its principal executive offices at 2830 De La Cruz Boulevard, Santa Clara, CA 95050.

## RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

## STATUS OF CLAIMS

Claims 1-73 are rejected, pending and appealed herein.

## STATUS OF AMENDMENTS

No Amendment has been filed subsequent to final rejection.

## SUMMARY OF INVENTION

One aspect of the invention is a method (e.g., 800 in FIG. 8) for distributing protected material. The method comprises ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient (e.g., 811~812 of FIG. 8 as described on page 18, lines 5~30); and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms (e.g., 813~818 of FIG. 8 as described on page 18, line 21 to page 19, line 12).

Another aspect is an apparatus (e.g., 600 of FIG. 6 or 700 of FIG. 7) for distributing protected material. The

apparatus includes a computer (e.g., distribution server 601 of FIG. 6; or the distribution server 701 of FIG. 7) having a first set of program code. The first set of program code serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient (e.g., 811~812 of FIG. 8 as described on page 18, lines 5~30). The first set of program code also thereupon serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms (e.g., 813~818 of FIG. 8 as described on page 18, line 21 to page 19, line 12).

Another aspect is a computer implemented method (e.g., 1000 of FIG. 10) for generating a database of unauthorized copying of protected material. The method comprises: detecting at least one identification embedded in a copy of protected material procured from a distribution channel (e.g., 1001~1006 of FIG. 10 as described on page 23, line 19 to page 24, line 13); and storing information of the protected material according to the at least one identification in a database so as to be indicative of unauthorized copying of the protected material (e.g., 1007~1011 of FIG. 10 as described on page 24, line 14-28).

Another aspect is an apparatus (e.g., 900 of FIG. 9) for generating a database of unauthorized copying of protected material (e.g., database 904 of FIG.9). The apparatus includes a computer (e.g., detection server 901 of FIG. 9) having a first set of program code. The first set of program code serves to detect at least one identification

embedded in a copy of protected material procured from a distribution channel (e.g., 1001~1006 of FIG. 10 as described on page 23, line 19 to page 24, line 13), and store information of the protected material according to the at least one identification in a database so as to be indicative of unauthorized copying of the protected material (e.g., 1007~1011 of FIG. 10 as described on page 24, line 14-28).

Still another aspect is an system (e.g., 1100 of FIG. 11; or 1200 of FIG. 12) for distributing protected material, and detecting unauthorized copying of such material. The system includes a detection server (e.g., detection server 1116 of FIG. 11; or detection server 1214 of FIG. 12) having a first program for detecting identifications embedded in copies of protected materials procured from at least one distribution channel (e.g., 1001~1006 of FIG. 10 as described on page 23, line 19 to page 24, line 13), and storing information of the protected materials according to the identifications in a database so as to be indicative of unauthorized copying of the protected material (e.g., 1007~1011 of FIG. 10 as described on page 24, line 14-28). The system also includes a distribution server (e.g., distribution server 1101 of FIG. 11; or publisher computer 1201 of FIG. 12) having a second program for ascertaining terms for providing a copy of a protected material to a prospective recipient according at least in part to the information in the database (e.g., 811~812 of FIG. 8 as described on page 18, lines 5~30), and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms (e.g.,

813~818 of FIG. 8 as described on page 18, line 21 to page 19, line 12).

## ISSUES

In the Final Rejection of July 21, 2004, claims 1-73, the claims on appeal, were rejected as being unpatentable under 35 U.S.C. §102(e) over U.S. Patent No. 6,381,747 issued to Wonfor et al. ("Wonfor et al."), and also, unpatentable under 35 U.S.C. §102(e) over U.S. Patent No. 6,438,235 issued to Sims III ("Sims III"). The Examiner contends, in effect, that appellant's invention is anticipated by both of these cited prior art references.

The issues can be succinctly stated as follows:

1. Whether Claims 1-73 are anticipated by U.S. Pat. No. 6,381,747 issued to Wonfor et al., and therefore, properly rejected as being unpatentable under 35 U.S.C. §102(e).

2. Whether Claims 1-73 are anticipated by U.S. Pat. No. 6,438,235 issued to Sims III, and therefore, properly rejected as being unpatentable under 35 U.S.C. §102(e).

## GROUPING OF CLAIMS

Claims 1-73 do not stand or fall together as explained in the Argument that follows.

## ARGUMENT

Applicant claims various aspects of a method and apparatus for determining the terms upon which audio-visual content is to be distributed to prospective recipients, wherein the terms take into account previously detected unauthorized copying of content (i.e., piracy history) by those recipients.

It is a unique feature of Applicant's invention that it adjusts the licensing terms for providing content to prospective recipients according to detected levels of prior unauthorized copying activity by those prospective recipients. See, e.g., page 14, lines 1-16.

Neither Wonfor et al. or Sims III performs such a function.

Wonfor et al. teaches a copy protection method and system directed towards protecting pay per view ("PPV") and/or pay to tape ("PTT") cable or satellite program transmissions to set top boxes in consumer homes. The set top boxes include a copy protection circuit which is adapted to apply selected anti-copy waveforms to the video signal corresponding to the program material. See, e.g., Abstract. In the event that a subscriber records the PPV protected program via a VCR to obtain a taped copy without authorization, the unauthorized copy will be degraded to the degree that it is unwatchable. See, e.g., Col. 5, lines 50-53.

In Wonfor et al., the set top boxes return usage information to a video service provider's control and billing (tracking) center for billing the subscriber for the PPV or PTT transaction usage. See, e.g., Col. 5, lines 15-24. The reference does not teach or even suggest, however, that such billing is modified according to any detected levels of unauthorized copying by subscribers. Further, it does not even attempt to detect unauthorized copying activity of other material previously provided to the subscribers since its copy protection system is intended to prevent such activity from occurring in the first place.

Sims III teaches a system and method for providing protection of content. In Sims III, the protected content is stored on a bulk storage media. Protection is provided in this case by a means through which the media is securely identified as being original and a playback device is securely identified as being authorized. As a consequence, devices or users of the media may be assured that interaction therewith is authorized as each end can securely identify the other and each end can securely send data to the other end. See, e.g., col. 3, lines 24-34.

Thus, neither Wonfor et al. or Sims III teach or even suggest a mechanism to adjust the licensing terms for providing content to prospective recipients according to detected levels of prior unauthorized copying activity by those prospective recipients. Wonfor et al. and Sims III merely teach copy protection mechanisms, wherein Wonfor et al. degrades any unauthorized copies so that they are

virtually unwatchable and Sims III prevents their creation in the first place.

Applicants' approach to providing protected material is radically different from such conventional copy protection techniques. Applicants' approach uses a prospective recipient's "piracy history" (i.e., information of unauthorized copying of other protected material previously provided to the prospective recipient) to ascertain the terms under which protected material being requested by the prospective recipient is provided to the prospective recipient.

Both Wonfor et al. and Sims III are essentially preventative approaches, whereas applicant's approach is more appropriately referred to as being compensatory for prior piracy activities conducted by a prospective recipient of protected material.

It is well established that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. See, e.g., Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

As will be explained in the following, there are elements in each of the stand-alone claims that are neither taught nor suggested by Wonfor et al. or Sims III, alone or in combination.

**Claim 1**

Claim 1 includes the element of "ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient."

In order to anticipate this element of the claim, the unauthorized copying must be of "other protected material" (i.e., not the material for which the terms are being ascertained), and the other protected material must have been "previously provided" to the prospective recipient (i.e., not provided concurrently with or after the material for which the terms are being ascertained).

Both Wonfor et al. and Sims III fail to teach this element of Claim 1.

As previously explained, Wonfor et al. merely frustrates attempts to make unauthorized copies by degrading the quality of those copies to the degree that they are unwatchable. Wonfor et al. makes no teaching or suggestion of "ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient."

As for Sims III, it prevents the unauthorized copying from occurring in the first place. As stated in Sims III, "Operation of the present invention is not to allow or

disallow any particular transmission, but rather to obscure the content (information or data), using cryptographic methods, such that only a legitimate recipient can make use of that data, i.e., nobody but the content owner, or those authorized by him/her, is able to copy protected media content." See, Col. 3, lines 34-40.

Thus, Sims III also makes no teaching or suggestion of "ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient."

Accordingly, Claim 1 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest "ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient."

**Claim 2**

Claim 2 includes the element of "obtaining said information of unauthorized copying from a database," and such a database and the obtaining of information from it are neither taught nor suggested by either Wonfor et al. or Sims III, alone or in combination with each other.

Accordingly, Claim 2 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest the element of "obtaining said information of unauthorized copying from a database".

**Claim 7**

Claim 7 includes the element of "embedding an identification of said prospective recipient in said copy prior to providing said copy to said prospective recipient," and such an element is neither taught nor suggested by either Wonfor et al. or Sims III, alone or in combination with each other.

It is noted herein that although Wonfor et al. discusses use of a password that a service provider specifies to limit access by its employees to modify copy protection (see, e.g., col. 7, lines 18-67, col. 8, lines 1-8), such a password is not identification of the prospective recipient (i.e., subscriber), nor is it embedded in the copy prior to providing the copy to the respective recipient.

It is also noted herein that although Sims III discloses a list of "acceptable users" included on the media, such a list is not an identification of a prospective recipient of the media. The list is instead a list of manufacturer's playback devices that are licensed or authorized to utilize the media. See, e.g., Col. 14, lines 35-40. Unlike the identification of the prospective recipient, such a list is

useless for identifying or detecting any unauthorized copying by the prospective recipient.

Accordingly, Claim 7 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest the element of "embedding an identification of said prospective recipient in said copy prior to providing said copy to said prospective recipient".

**Claim 15**

Claim 15 includes the element of "determining a price for providing said protected material to said prospective recipient according to a formula and information of unauthorized copying of other protected material previously provided to said prospective material," and such an element is neither taught nor suggested by either Wonfor et al. or Sims III, alone or in combination with each other.

Accordingly, Claim 15 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest the element of "determining a price for providing said protected material to said prospective recipient according to a formula and information of unauthorized copying of other protected material previously provided to said prospective material".

**Claim 41**

Claim 41 claims a method for generating a database of unauthorized copying of protected material, and such method is neither taught nor suggested by either Wonfor et al. or Sims III, alone or in combination with each other. In particular, both Wonfor et al. and Sims III do not even detect unauthorized copying activity of other material previously provided to the subscribers since their copy protection systems are intended to prevent such activity from occurring in the first place.

More particularly, Claim 41 includes the elements of "detecting at least one identification embedded in a copy of protected material procured from a distribution channel, and storing information of said protected material according to said at least one identification in a database so as to be indicative of unauthorized copying of said protected material" and such elements are neither taught nor suggested by either Wonfor et al. or Sims III, alone or in combination with each other.

Accordingly, Claim 41 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest the elements of "detecting at least one identification embedded in a copy of protected material procured from a distribution channel, and storing information of said protected material according to said at least one identification in a database so as to be indicative of unauthorized copying of said protected material".

**Claim 63**

Claim 63 claims an apparatus for distributing protected material, comprising: a detection server having a first program for detecting identifications embedded in copies of protected materials procured from at least one distribution channel, and storing information of said protected materials according to said identifications in a database so as to be indicative of unauthorized copying of said protected material; and a distribution server having a second program for ascertaining terms for providing a protected material to a prospective recipient according at least in part to said information in said database, and providing or withholding a copy of said protected material to said prospective recipient in accordance with said terms.

As previously explained respectively in reference to Claims 1 and 41, such functions as performed by the detection server and distribution server are neither taught nor suggested by Wonfor et al. or Sims III, alone or in combination, and therefore, the detection and distribution servers as claimed in Claim 63 are also neither taught nor suggested by these references.

Accordingly, Claim 63 is believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since neither of these references teaches each and every element of the claim and in particular, teach or suggest the elements of a "detection server" or "distribution server" as claimed.

**Related Claims**

Claims 2-20 are also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since they depend from Claim 1, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 1.

Claim 21 is an apparatus claim paralleling aspects of the method of Claim 1. Accordingly, Claim 21 is also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III for the same reasons as stated in reference to Claim 1.

Claims 22-40 are also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since they depend from Claim 21, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 21.

Claims 42-51 are also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since they depend from Claim 41, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 41.

Claim 52 is an apparatus claim paralleling aspects of the method of Claim 41. Accordingly, Claim 52 is also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III for the same reasons as stated in reference to Claim 41.

Claims 53-62 are also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since they depend from Claim 52, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 52.

Claims 64-73 are also believed to be patentable under 35 U.S.C. 102(e) over Wonfor et al. and Sims III since they depend from Claim 63, and as such, are believed to be patentable for at least the same reasons as stated in reference to Claim 63, as well as other reasons as stated in reference to Claim 7 and 15, as appropriate.

## CONCLUSIONS

To summarize, appellant submits that all the claims on appeal are patentable because neither Wonfor et al. or Sims III teach or suggest all of the elements of Claims 1-73, alone or in combination with each other, for the reasons stated in the Arguments above.

Although it is noted in various places above that Wonfor et al. not only fails to teach the various aspects of the present invention, but also, it fails to suggest such aspects, even if Wonfor et al. did arguably suggest any such aspects, use of Wonfor et al. in a 35 U.S.C. 103(a) rejection would be inappropriate according to 35 U.S.C. 103(c) since the present invention and that of Wonfor et al. was commonly owned at the time the invention was made.

If the Board agrees with the statements submitted above, they should allow all the claims on appeal.

Accordingly, the reversal of the Examiner by the honorable Board of Appeals is respectfully solicited.

Respectfully submitted,

Dated: August 31, 2004

Victor H. Okumoto
Registration No. 35,973
Attorney for Appellant
(510) 792-1112

## APPENDIX

Following is a copy of the claims involved in the appeal.

1. A computer implemented method for distributing protected material, comprising:

ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient; and

providing or withholding a copy of said protected material to said prospective recipient in accordance with said terms.

2. The method according to claim 1, wherein said ascertaining further includes obtaining said information of unauthorized copying from a database.

3. The method according to claim 1, wherein said providing comprises providing a copy of said protected material to said prospective recipient in the form of a file.

4. The method according to claim 1, wherein said providing comprises providing a copy of said protected material to said prospective recipient in the form of streaming media.

5. The method according to claim 4, wherein said protected material includes audio-visual content.

6. The method according to claim 5, further comprising embedding an identification of said protected material in said copy prior to providing said copy to said prospective recipient.

7. The method according to claim 5, further comprising embedding an identification of said prospective recipient in said copy prior to providing said copy to said prospective recipient.

8. The method according to claim 7, wherein said embedding employs a steganographic technique.

9. The method according to claim 7, wherein said embedding employs a watermarking technique.

10. The method according to claim 7, wherein said identification of said prospective recipient includes a credit card number of said prospective recipient.

11. The method according to claim 7, wherein said identification of said prospective recipient includes an electronic signature of said prospective recipient.

12. The method according to claim 7, wherein said identification of said prospective recipient includes a serial number associated with a computer of said prospective recipient.

13. The method according to claim 7, wherein said identification of said prospective recipient includes

an Internet protocol address associated with a network interface card in a computer of said prospective recipient.

14. The method according to claim 7, further comprising encrypting said protected material in said copy of said protected material prior to providing said copy to said prospective recipient.

15. The method according to claim 7, wherein said ascertaining comprises determining a price for providing said protected material to said prospective recipient according to a formula and information of unauthorized copying of other protected material previously provided to said prospective recipient.

16. The method according to claim 15, further comprising receiving an identification of said protected material and said identification of said prospective recipient over the Internet, and said providing of said copy of said protected material to said prospective recipient employs the Internet.

17. The method according to claim 15, wherein said ascertaining comprises:

transmitting said identification of said prospective recipient to a remote server; and

receiving said terms for providing said protected material to said prospective recipient back from said remote server.

18. The method according to claim 17, wherein said providing comprises:

recording said copy of said protected material on a tangible medium; and

providing said tangible medium to said prospective recipient according to said terms.

19. The method according to claim 18, wherein said tangible medium is a compact disc.

20. The method according to claim 18, wherein said tangible medium is a digital versatile disc.

21. An apparatus for distributing protected material, comprising a computer having a first set of program code for:

ascertaining terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to said prospective recipient; and

providing or withholding a copy of said protected material to or from said prospective recipient in accordance with said terms.

22. The apparatus according to claim 21, wherein said ascertaining further includes obtaining said information of unauthorized copying from a database.

23. The apparatus according to claim 21, wherein said providing comprises providing a copy of said protected material to said prospective recipient in the form of a file.

24. The apparatus according to claim 21, wherein said providing comprises providing a copy of said protected material to said prospective recipient in the form of streaming media.

25. The apparatus according to claim 24, wherein said protected material includes audio-visual content.

26. The apparatus according to claim 25, wherein said computer has a second set of program code for embedding an identification of said protected material in said copy prior to providing said copy to said prospective recipient.

27. The apparatus according to claim 26, wherein said computer has a second set of program code for embedding an identification of said prospective recipient in said copy prior to providing said copy to said prospective recipient.

28. The apparatus according to claim 27, wherein said embedding employs a steganographic technique.

29. The apparatus according to claim 27, wherein said embedding employs a watermarking technique.

30. The apparatus according to claim 27, wherein said identification of said prospective recipient includes a credit card number of said prospective recipient.

31. The apparatus according to claim 27, wherein said identification of said prospective recipient includes an electronic signature of said prospective recipient.

32. The apparatus according to claim 27, wherein said identification of said prospective recipient includes a serial number associated with a computer of said prospective recipient.

33. The apparatus according to claim 27, wherein said identification of said prospective recipient includes an Internet protocol address associated with a network interface card in a computer of said prospective recipient.

34. The apparatus according to claim 27, wherein said computer has a third set of program code for encrypting said protected material in said copy prior to providing said copy to said prospective recipient.

35. The apparatus according to claim 27, wherein said ascertaining comprises determining a price for providing said protected material to said prospective recipient according to a formula and information of unauthorized copying of other protected material previously provided to said prospective recipient.

36. The apparatus according to claim 35, wherein said first set of program code is further for receiving an identification of said protected material and said identification of said prospective recipient over the Internet, and said providing of said copy of said protected

material to said prospective recipient employs the Internet.

37. The apparatus according to claim 35, wherein said ascertaining comprises:

transmitting said identification of said prospective recipient to a remote server; and

receiving said terms for providing said protected material to said prospective recipient back from said remote server.

38. The apparatus according to claim 37, wherein said providing comprises:

recording said copy of said protected material on a tangible medium; and

providing said tangible medium to said prospective recipient according to said terms.

39. The apparatus according to claim 38, wherein said tangible medium is a compact disc.

40. The apparatus according to claim 38, wherein said tangible medium is a digital versatile disc.

41. A computer implemented method for generating a database of unauthorized copying of protected material, comprising:

detecting at least one identification embedded in a copy of protected material procured from a distribution channel; and

storing information of said protected material according to said at least one identification in a database

so as to be indicative of unauthorized copying of said protected material.

42. The method according to claim 41, wherein said at least one identification includes a content identification identifying said protected material, and a recipient identification identifying a recipient of said protected material.

43. The method according to claim 42, wherein said at least one identification has been embedded in said protected material by a steganographic technique.

44. The method according to claim 42, wherein said at least one identification has been embedded in said protected material by a watermarking technique.

45. The method according to claim 42, wherein said protected material includes audio-visual content.

46. The method according to claim 45, wherein said recipient is an original purchaser of said copy of said protected material.

47. The method according to claim 46, wherein said recipient identification is a credit card number of said original purchaser.

48. The method according to claim 45, wherein said recipient is an independent contractor involved in post-production work on said protected material.

49. The method according to claim 45, further comprising procuring said copy of said protected material over the Internet.

50. The method according to claim 49, wherein said procuring comprises:

contacting a list server; and

downloading a copy of a selected protected material from an on-line client identified by said list server.

51. The method according to claim 49, wherein said procuring comprises:

searching for a selected protected material; and

downloading a coy of said selected protected material from an on-line client identified as a result of said searching.

52. An apparatus for generating a database of unauthorized copying of protected material, comprising a computer having a first set of program code for:

detecting at least one identification embedded in a copy of protected material procured from a distribution channel; and

storing information of said protected material according to said at least one identification in a database so as to be indicative of unauthorized copying of said protected material.

53. The apparatus according to claim 52, wherein said at least one identification includes a content identification identifying said protected material, and a

recipient identification identifying a recipient of said protected material.

54. The apparatus according to claim 53, wherein said at least one identification has been embedded in said protected material by a steganographic technique.

55. The apparatus according to claim 53, wherein said at least one identification has been embedded in said protected material by a watermarking technique.

56. The apparatus according to claim 53, wherein said protected material includes audio-visual content.

57. The apparatus according to claim 56, wherein said recipient is an original purchaser of a copy of said protected material.

58. The apparatus according to claim 57, wherein said recipient identification is a credit card number of said original purchaser.

59. The apparatus according to claim 56, wherein said recipient is an independent contractor involved in post-production work on said protected material.

60. The apparatus according to claim 56, wherein said computer has a second set of program code for procuring said protected material over the Internet.

61. The apparatus according to claim 60, wherein said procuring comprises:

contacting a list server; and

downloading a copy of a selected protected material from an on-line client identified by said list server.

62. The apparatus according to claim 60, wherein said procuring comprises:

searching for a selected protected material; and

downloading a copy of said selected protected material from an on-line client identified as a result of said searching.

63. An apparatus for distributing protected material, comprising:

a detection server having a first program for detecting identifications embedded in copies of protected materials procured from at least one distribution channel, and storing information of said protected materials according to said identifications in a database so as to be indicative of unauthorized copying of said protected material; and

a distribution server having a second program for ascertaining terms for providing a protected material to a prospective recipient according at least in part to said information in said database, and providing or withholding a copy of said protected material to said prospective recipient in accordance with said terms.

64. The apparatus according to claim 63, wherein said protected material includes audio-visual content.

65. The apparatus according to claim 64, wherein said distribution server has a third program for embedding an identification of said protected material in said copy prior to providing said copy to said prospective recipient.

66. The apparatus according to claim 65, wherein said third program is further for embedding an identification of said recipient in said copy prior to providing said copy to said prospective recipient.

67. The apparatus according to claim 66, wherein said embedding employs a steganographic technique.

68. The apparatus according to claim 66, wherein said embedding employs a watermarking technique.

69. The apparatus according to claim 64, wherein said ascertaining comprises determining a price for providing said protected material to said prospective recipient according to a formula and said information in said database.

70. The apparatus according to claim 69, wherein said second program is further for receiving a content identification of said protected material and a recipient identification of said prospective recipient over the Internet, and said providing of said copy employs the Internet.

71. The apparatus according to claim 64, wherein said detection server has a fourth program for procuring

said protected material from at least one distribution channel over the Internet.

72. The apparatus according to claim 71, wherein said procuring comprises:

contacting a list server; and

downloading selected protected materials from on-line clients identified by said list server.

73. The apparatus according to claim 71, wherein said procuring comprises:

searching for selected protected materials; and

downloading said selected protected materials from on-line clients identified as a result of said searching.